CHAPTER

8

MANAGING ACCOUNTS AND CLIENT CONNECTIVITY

After reading this chapter and completing the exercises you will be able to:

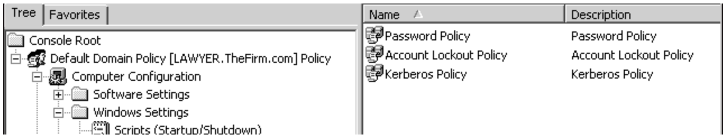
- Establish account naming conventions
- Configure account security policies
- Create and manage accounts, including setting up a new account, configuring account properties, delegating account management, and renaming, disabling, and deleting an account
- Create local user profiles, roaming profiles, and mandatory profiles
- Configure client network operating systems to access Windows 2000 Server, and install client operating systems through Remote Installation Services

Clients are the reason for a server's existence. A server makes networking meaningful to clients because it gives clients access to all kinds of valuable resources such as files, databases, printers, Web information, and software. Providing client access to servers is the single largest reason for the worldwide explosive growth in networks. Windows 2000 Server is a particularly versatile server because it hosts a large range of clients from MS-DOS to Windows 2000 Professional to Macintosh and UNIX.

You have already started learning how to configure Windows 2000 Server for all types of clients by setting up protocols that include TCP/IP, NWLink, AppleTalk, NetBEUI, and DLC. In this chapter, you take the next step by learning how to establish a naming convention for accounts and how to configure account policies to help keep a network secure. You also learn to configure and manage accounts, including creating user profiles. Finally, you learn how to set up different client network operating systems to connect to Windows 2000 Server, and how to configure Windows 2000 Server for those clients.

SETTING UP ACCOUNT NAMING CONVENTIONS

Users access network servers and resources through accounts. Before establishing accounts, organizations set up account names based on the account user's actual name or function within the organization. For example, if the organization uses the users' actual names, it will adopt a particular naming convention, because it is clumsy to use the full names. Also, server storage for the full name is limited by the operating system. Some IBM mainframe operating systems limit the length of the username to eight characters. Windows 2000 Server limits user account names to 20 characters that include letters, numbers, and some symbols.



Console Root
Default Domain Policy [LAWYER.TheFirm.com] Policy
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdown)

Name	Description
Password Policy	Password Policy
Account Lockout Policy	Account Lockout Policy
Kerberos Policy	Kerberos Policy

Some conventions for account names based on the user's actual name are as follows:

- Last name followed by the initial of the first name (PalmerM)
- First name initial followed by the last name (MPalmer)
- First name initial, middle initial, and last name (MJPalmer)

When an organization creates usernames by position or function, it often uses descriptive names. For example, the payroll office may use the names Paysuper (payroll supervisor), Payclerk (payroll clerk), and Payassist (payroll assistant). Another example is the names that schools give to accounts in student labs, such as Lab1, Lab2, Lab3, and so on. The advantage of naming accounts by function is that an account does not have to be purged when the account holder leaves or changes positions. The network administrator simply changes the account password, and gives it to the new person in that position. The advantage of having accounts based on the user's name is that it is easier to know who is logged on to a server (if the naming convention is well designed).

TIP In a large organization where computer systems and software are audited by independent financial auditors, the auditors often prefer to have accounts named for individual users. This provides the best audit tracking of who has made what changes to data.

ESTABLISHING ACCOUNT POLICIES

Account policies are security measures set up in a group policy that applies to all accounts or to all accounts in a container, such as a domain, when the Active Directory is installed (see Chapter 4). The account policy options affect two main areas, password security and account lockout. Another option is to use Kerberos security. There is no requirement to implement these security options, but most server administrators choose to use them. Many organizations like to have some guidelines to help computer users take advantage of computer security features to protect company information from people inside or outside the organization who could misuse it. Security features also protect the server and printer resources from malicious activities.

The first line of defense for Windows 2000 Server is password security, but it is only effective if users are taught to use it properly. Many users are careless about security, viewing it as an impediment to their work. They may tape passwords inside a desk drawer or use easily guessed passwords, such as the first name of a family member. Some users keep the same password for months or years, even though it may become known to several other people. Systems like Windows 2000 Server have built-in capabilities to help users become more conscious of maintaining passwords. One option is to set a password expiration period, requiring users to change passwords at regular intervals. Many organizations use this feature, for example requiring that users change their passwords every 45 to 90 days.

> TIP Server administrators should consider changing passwords every month for the Administrator account and other accounts that can access sensitive information.

Some organizations require that all passwords have a minimum length, such as six or seven characters. This requirement makes passwords more difficult to guess. Another option is to have the operating system "remember" passwords that have been used previously. For example, the system might be set to recall the last five passwords, preventing a user from repeating one of these. Password recollection forces the user to change to a different password instead of reusing the same one when a new one is set. Windows 2000 Server is capable of monitoring unsuccessful logon attempts, in case an intruder attempts to break into an account by trying various password combinations. The operating system can employ account lockout to lock out an account (including the true account owner) after a number of unsuccessful tries. The lockout can be set to release after a specified period of time or by intervention from the server administrator. For example, at one university, a part-time custodian who had keys to computer center staff offices attempted to access the Administrator accounts on servers at night. Account lockout prevented him from accessing those sensitive accounts until his surreptitious activities were discovered and stopped.

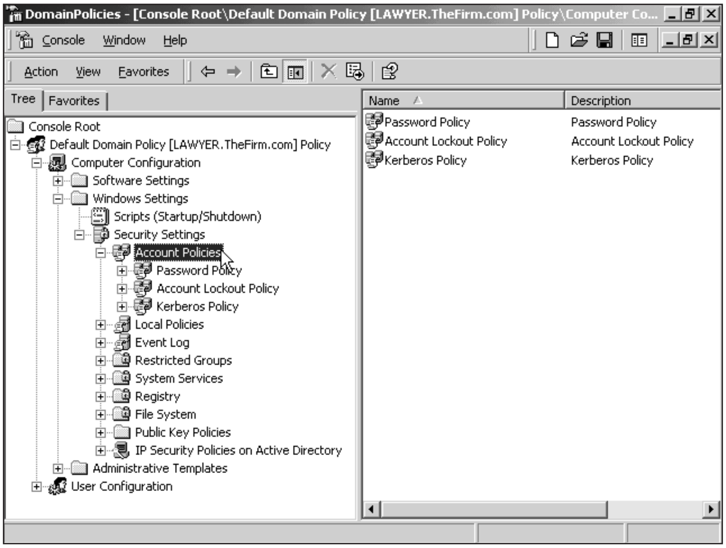
A common policy is to have lockout go into effect after five to ten unsuccessful logon attempts. Also, an administrator can set lockout to release after a designated time, such as 30 minutes. The 30 minutes creates enough delay to discourage intruders, while giving some leeway to a user who might have forgotten a recently changed password.

Kerberos security involves the use of tickets that are exchanged between the client who requests logon and network services access and the server or Active Directory that grants access. On a network that does not use the Active Directory, each standalone Windows 2000 server can be designated as a Kerberos key distribution center, which means that the server stores user accounts and passwords. When the Active Directory is used, then each domain controller is a key distribution center. When a user logs on, the client computer sends an account name and password to the key distribution center. The key distribution center responds by issuing a temporary ticket that grants the user access to the Kerberos ticket-granting service on a domain controller (or standalone server), which then grants a permanent ticket to that computer. The permanent ticket, called a **service ticket**, is good for the duration of a logon session (or for another period of time specified by the server administrator in the account polices) and enables the computer to access network services beginning with the Logon service. The permanent ticket contains information about the account that is used to identify the account to each network service it requests to use. You might think of a Kerberos ticket as similar to one you would purchase to enter a concert; the ticket is good for the duration of that event and for entry to refreshment and merchandise booths, but you must purchase a new ticket to attend a concert on another date.

Configuring account policies is accomplished through the MMC Group Policy snap-in. You can add the snap-in by using these steps:

1. Start MMC from the Start button, Run option, click the MMC Console menu, and click Add/Remove Snap-in.
2. In the Add/Remove Snap-in dialog box, click Add, scroll to Group Policy, and double-click it.
3. When the Select Group Policy Object Wizard starts, choose Local Computer, if you have not installed the Active Directory, and click Finish. If you have installed the Active Directory, click the Browse button, double-click Default Domain Policy, and click Finish.
4. Click Close and click OK.

The account policies are located in the Computer Configuration management category as part of the Windows Settings. For example, to access the domain-wide policies when the Active Directory is installed, in the left pane double-click Default Domain Policy, Computer Configuration, Windows Settings, Security Settings, and Account Policies, which will display the window shown in Figure 8-1.



Name	Description
Password Policy	Password Policy
Account Lockout Policy	Account Lockout Policy
Kerberos Policy	Kerberos Policy

Figure 8-1 Account policies

Double-click Password Policy in the left or right pane to view the security options. To change an option, double-click that option and make the change in the dialog box that is displayed. The options are the following:

- *Enforce password history:* Enables you to require users to choose new passwords when they make a password change, because the system can remember the previously used passwords
- *Maximum password age:* Permits you to set the maximum time allowed until a password expires
- *Minimum password age:* Permits you to specify that a password must be used for a minimum amount of time before it can be changed
- *Minimum password length:* Enables you to require that passwords are a minimum length
- *Passwords must meet complexity requirements:* Enables you to create a filter of customized password requirements that each account password must follow
- *Store password using reversible encryption for all users in the domain:* Enables passwords to be stored in reversible encrypted format

Double-click Account Lockout Policy in the left pane to configure the account lockout parameters, which include:

- *Account lockout duration:* Permits you to specify in minutes how long the system will keep an account locked out after reaching the specified number of unsuccessful logon attempts
- *Account lockout threshold:* Enables you to set a limit to the number of unsuccessful attempts to log on to an account
- *Reset account lockout count after:* Enables you to specify the number of minutes between two consecutive unsuccessful logon attempts, to make sure that the account will not be locked out too soon

When the Active Directory is installed, the account policies include the option to configure Kerberos, which is the default authentication. If the Active Directory is not installed, Kerberos is not included in the account policies because the default authentication is through **Windows NT LAN Manager** (**NTLM**). NTLM is the authentication used by all versions of Windows NT Server prior to Windows 2000 Server. To configure Kerberos in the Active Directory, double-click Kerberos Policy in the left pane to access the following parameters:

- *Enforce user logon restrictions:* Turns on Kerberos security, which is the default
- *Maximum lifetime for a service ticket:* Determines the maximum amount of time in minutes that a service ticket can be used to continually access a particular service in one service session

- *Maximum lifetime for a user ticket:* Determines the maximum amount of time in hours that a ticket can be used in one continuous session for access to a computer or domain
- *Maximum lifetime for user ticket renewal:* Determines the maximum number of days that the same Kerberos ticket can be renewed each time a user logs on
- *Maximum tolerance for computer clock synchronization:* Determines how long in minutes a client will wait until synchronizing its clock with that of the server or Active Directory it is accessing

As is true for password and lockout policies, any of the Kerberos policy parameters can be included or excluded. Server and client operating systems that support Kerberos include Windows 2000 Server and Windows 2000 Professional. It can also be used in non-Windows 2000 operating systems that have the Directory Service Client software installed (described later in this chapter).

> TIP
>
> If getting users to log off when they go home at night is a problem, limit the *maximum lifetime for service ticket* or *maximum lifetime for user ticket* values to a certain number of hours, such as 10 or 12.

When you set up account policies, there is a difference between setting policies for a server that is in a domain and setting them for a server that is not. For a server that is not in a domain, you set policies for that local server only. In contrast, when the Active Directory is installed, you set policies for all computers that are members of the domain (try Hands-on Project 8-1).

You can, however, create organizational units (OUs) and create policies that are applicable to each OU and that may be different from the policies for the domain. For example, you may want to tighten security for a particular OU, such as a group of user accounts in which the users are performing highly secret research. In this case, you might tighten password security to require 10 characters for that group, whereas the domain security might require only six. If you create special security policies for particular OUs, then use the Security Templates MMC snap-in to create specially named templates for each OU, and then apply each template to a group policy that is applicable to its OU.

Creating and Managing Accounts

With the account policies established, the next step is to create accounts. Two accounts, Administrator and Guest, are set up when you install Windows 2000 Server. Accounts that are created when the Active Directory is not installed or that are on a standalone server that is not part of a domain are local user accounts and can only be used on that individual server. When accounts are created in the domain through the Active Directory, then those accounts can be used to access any domain server or resource.

New accounts are set up by first installing the MMC Local Users and Groups snap-in for servers that do not use the Active Directory. When the Active Directory is installed and the server is a domain controller, use the MMC Active Directory Users and Computers snap-in. Each new account is created by entering account information and password controls.

Note

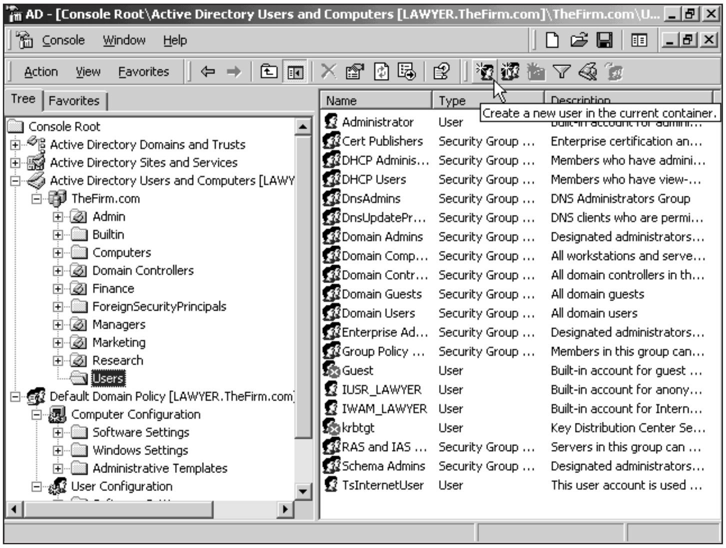
If you are using the Active Directory and are working on a DC, Windows 2000 Server will not allow you to install the Local Users and Groups snap-in, because you must use the Active Directory Users and Computers snap-in instead.

To create a local user account on a server that is not part of a domain:

1. Double-click Local Users and Groups in the MMC.
2. Click Users and then click the Action menu.
3. Click New User.

To create an account in the Active Directory:

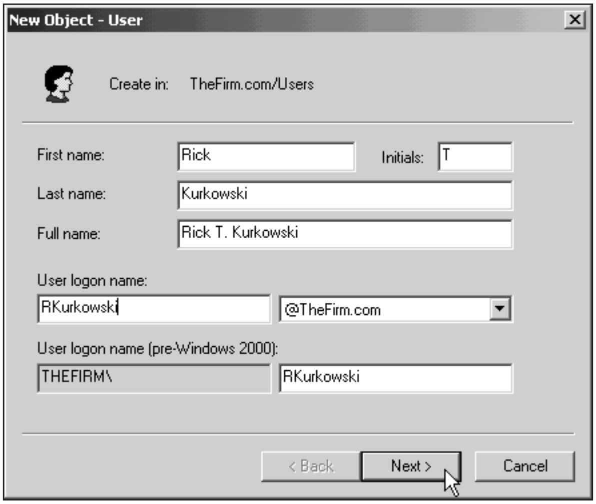
1. Double-click the Active Directory Users and Computers snap-in in the left pane, and double-click the domain name.
2. Click Users in the left-pane tree.
3. Click the *Create a new user in the current container* button, which is an icon resembling a single person, on the button bar (see Figure 8-2).


AD - [Console Root\Active Directory Users and Computers [LAWYER.TheFirm.com]\TheFirm.com\U...
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers [LAWY
TheFirm.com
Admin
Builtin
Computers
Domain Controllers
Finance
ForeignSecurityPrincipals
Managers
Marketing
Research
Users
Default Domain Policy [LAWYER.TheFirm.com]
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Create a new user in the current container.

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Enterprise certification an...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
IUSR_LAWYER	User	Built-in account for anony...
IWAM_LAWYER	User	Built-in account for Intern...
krbtgt	User	Key Distribution Center Se...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
TsInternetUser	User	This user account is used ...

Figure 8-2 Creating a new user in a domain

Complete the name, user logon name, password, password confirmation, and optional parameters in the dialog boxes used to create a new account (one dialog box for a local user account and two dialog boxes for a domain account). For example, to create an account in the Active Directory, enter the first name, middle initial, and last name of the user and provide the user logon name (see Figure 8-3). The domain name is provided automatically, as is a pre-Windows-2000 logon name for pre-Windows-2000 clients. Click Next to go to the next screen.


New Object - User

Create in: TheFirm.com/Users

First name: Rick
Initials: T
Last name: Kurkowski
Full name: Rick T. Kurkowski

User logon name:
RKurkowski @TheFirm.com

User logon name (pre-Windows 2000):
THEFIRM\ RKurkowski

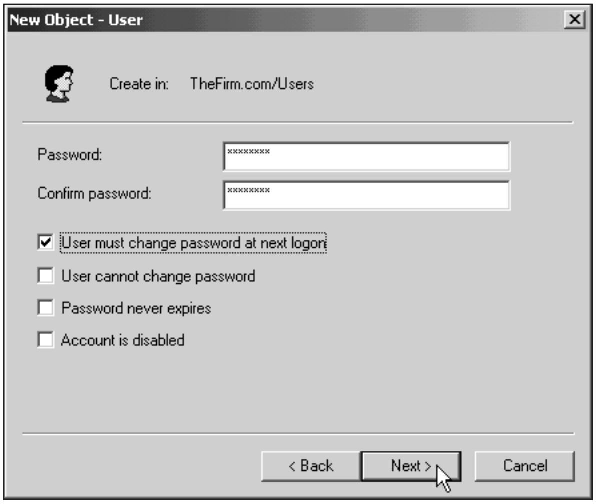
Figure 8-3 New user information

The next dialog box enables you to enter a password and confirm it for the account. Also, there are four parameters that enable you to control the account further. For example, the *User must change password at next logon* option forces users to enter a new password the first time they log on. This option is unnecessary for accounts used by the server administrator, but it is valuable for accounts created for others. Server administrators check this box when creating new accounts so that they will not know the passwords of account holders. Although the initial password is known, once it is given to the account holder, the administrator will not know the new password that the user is forced to enter at first logon.

Another option is to check *User cannot change password*, which means that only the network administrator can assign the password to an account. Under most circumstances, it is best for users to create their own confidential passwords, so they are the only ones using their accounts. Confidential passwords provide good security and ensure that if an account is audited, the activities audited are only those of the account holder. However, this option is used for special accounts, such as one that is used by the Windows 2000 Replicator for automatically copying files from one server to another server. Two other accounts for which the administrator may want to control the passwords are the Guest account and accounts used to access Internet Information Services.

The option *Password never expires* is used in some situations in which an account must always be accessed, even if no one remembers to change the password. That would be true for a utility account needed to run a program process. The password would be hard-coded into the program for the purpose of accessing the account to start the process. For example, you might create an account that automatically copies database files twice a day, which is done in client/server environments where one database is used for updating information throughout the day. A copy of the database is made, for example each morning and each afternoon, and is used for creating reports on the data. That way, heavy demand from large reports never slows down database updating, because reports are generated from the separate, copied database.

The *Account is disabled* option is used to stop activity on an account after the account holder leaves the organization. For example, if the payroll supervisor decides to go on a leave of absence for two months, the administrator might disable his or her account for that time period. That would secure the account until the supervisor's return. Figure 8-4 shows the New Object – User dialog box with the information entered for an account.



New Object - User

Create in: TheFirm.com/Users

Password: ********

Confirm password: ********

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

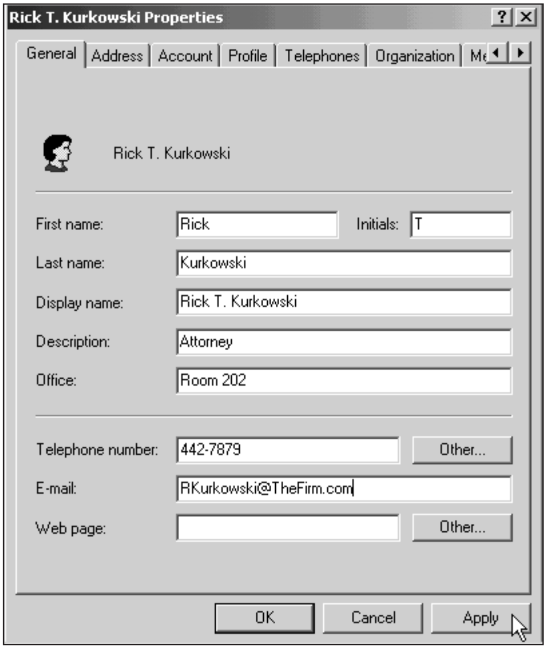
Figure 8-4 New user account parameters

After the parameters are entered, click Next to view a summary of the information you have entered, and then click Finish to create the account or click Back to reenter a parameter.

Note

If you are creating an account on a server on which the Active Directory is not installed, you would click Close instead of Finish after the parameters are entered, then double-click the newly created user account to access the account properties.

The next step is to double-click the account in the right pane, which displays user accounts and groups under Users, to further configure the properties associated with that account, as shown in Figure 8-5. (Try Hands-on Project 8-2 to create an account and to practice configuring account properties.)



Rick T. Kurkowski

First name: Rick Initials: T

Last name: Kurkowski

Display name: Rick T. Kurkowski

Description: Attorney

Office: Room 202

Telephone number: 442-7879 Other...

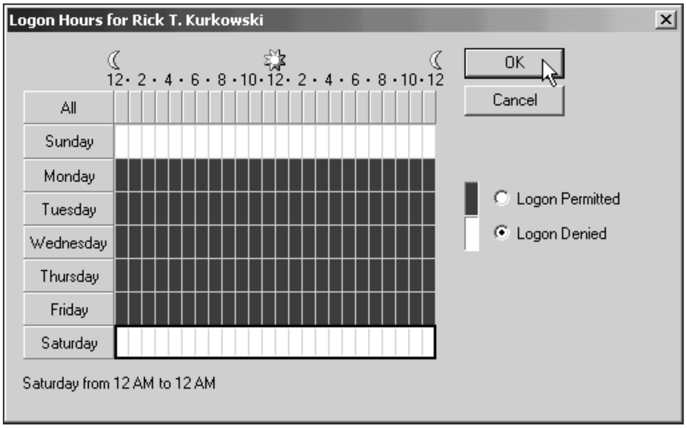
E-mail: RKurkowski@TheFirm.com

Web page: Other...

Figure 8-5 Account properties in the Active Directory

The account properties that you can set up are the following:

- *General tab:* Enables you to enter or modify personal information about the account holder that includes the first name, last name, name as it is displayed in the console, description of the user or account, office location, telephone number, e-mail address, and home page. There are also optional buttons to enter additional telephone numbers and Web page addresses for the account holder.
- *Address tab:* Used to provide information about the account holder's street address, Post Office box, city, state or province, postal code, and country or region.
- *Account tab:* Provides information about the logon name, domain name, account options such as requiring the user to change her or his password at next logon, and account expiration date, if one applies. For example, you can set an expiration date on an account when it is used by a temporary employee or when you know an employee's last day to work. There is also a button on this tab that enables you to set up an account so that the user cannot access the server at designated times, such as during backups and at times designated for system work on the server. For example, if your system work time is every Thursday evening from 8:00 to 10:00 p.m., you can reserve the server or domain so no one else can access it—or you may want to restrict accounts from accessing the server or domain over the weekend as a security measure when the office is closed. You do this by clicking the Logon Hours button on the Account tab. When the Logon Hours dialog box is displayed, block out the days and times when logon is denied, as in Figure 8-6. (Try Hands-on Project 8-2 to set server accessibility.)



Logon Hours for Rick T. Kurkowski

○ Logon Permitted
● Logon Denied

Saturday from 12 AM to 12 AM

Figure 8-6 Controlling account access by the day of the week and time

The Log On To button on the Account tab enables you to limit where a user can log on to the server or domain. The Log On To option is a good security measure when you want to make sure certain accounts can only be accessed from designated workstations. For example, you might want to guard the Administrator account and your own account with administrator privileges so they are only accessible from the server, from a workstation in your office, and from your computer at home. At the same time, the employee who prepares the payroll in your organization may be required by the auditors to finalize the payroll from one computer only. For example, suppose that the payroll is finalized from the payroll clerk's workstation, which is assigned the computer name PAY. Click the option *The following computers*, enter PAY as the workstation's name, click the Add button, and click OK.

- *Profile tab:* Enables you to associate a particular profile with a user or set of users, such as a common desktop (profiles are discussed later in this chapter). This tab also is used to associate a logon script and a home folder (directory) with an account. When home folders are set up on a server, administrators often standardize the home folder of all users to a particular drive letter, such as H. To enter the home folder drive letter, click the Connect radio button and use the list box to select the drive letter. Enter the path to the home folder in the To box, for example \Users\Kurkowski. Each time the user logs on, an H drive will be shown in My Computer and in Explorer, with a path to the user's home folder on the server. If the home folder is on the user's computer, click the Local path option and enter the computer name and the path on the computer to be used as a home folder, such as \\Mycomputer\Mywork\, using the **Universal Naming Convention** (**UNC**). The format for a UNC name is \\servername(or *computername*)*sharename**folder**file*. A **logon script** is a set of commands that automatically runs each time the user logs on to the server or domain. It is usually implemented as a DOS batch file, but it can also be an executable file. A summary of the commands is provided in Table 8-1.

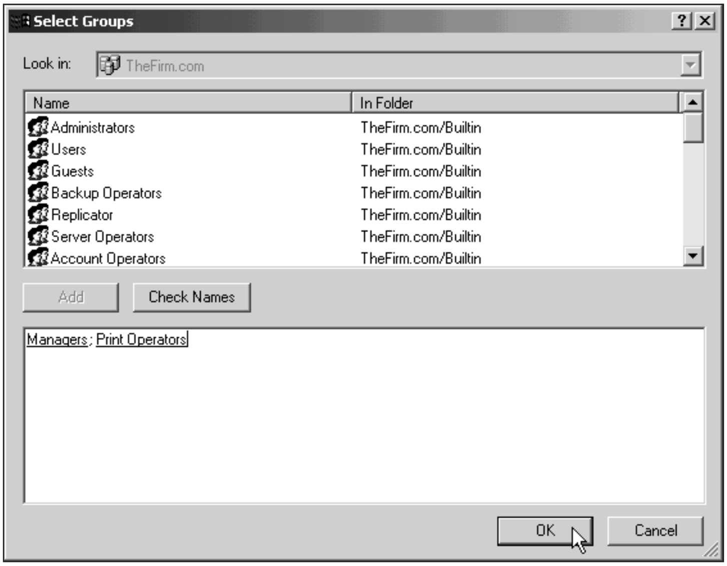
Table 8-1 Windows 2000 Server Logon Script Commands

Script Command	Function
%Homepath%	Establishes the path to the user's home folder
%Homedrive%	Sets a drive letter for the system hard disk drive
%Username%	Specifies the user's logon name
%Userdomain%	Specifies the domain to which the user belongs
%OS%	Specifies the operating system being used
%Processor%	Specifies the type of processor
%Homeshare%	Specifies a home directory on a shared drive

- *Telephones tab:* Enables you to associate specific types of telephone contact numbers for an account holder, which include one or more numbers for home, pager, mobile, fax, and IP phones. You can also enter particular comments, such as "Call the pager number only between 5 p.m. and midnight."

- *Organization tab:* Provides a place to enter the account holder's title, department name, company name, and the name of the person who manages the account, if it is not the administrator. There is also a box that lists other accounts that are managed by this account.

- *Member Of:* Used to add the account to an existing group of users. Accounts that have the same security and access requirements can be assigned as members of a group. Security access then is set up for the group instead of for each account. User groupings can save a significant amount of time when there are tens or hundreds of accounts to manage. For example, if 42 accounts all need full access to a folder, it is easier to create a group, add each account to the group, and give the group full access. The more time-consuming method would be to set up access permissions on individual accounts, repeating the same steps 42 times. To place an account in a group, click the Add button on the Member Of tab and double-click the group among the list of groups displayed in the Select Groups dialog box (see Figure 8-7). You can add the account to one or more groups using this procedure and then click OK when you are finished (security groups are discussed in Chapter 9). The Set Primary Group button on the Member Of tab is used to designate a primary group membership for accounts that are accessed by a Macintosh or POSIX client. Windows 2000 Server requires these systems to log on as members of a **primary group**, which is a global security group (see Chapter 9) that can access any server in a domain. To set a primary group, first add the group, click it in the Member of box, and click Set Primary Group.



Look in: TheFirm.com

Name	In Folder
Administrators	TheFirm.com/Builtin
Users	TheFirm.com/Builtin
Guests	TheFirm.com/Builtin
Backup Operators	TheFirm.com/Builtin
Replicator	TheFirm.com/Builtin
Server Operators	TheFirm.com/Builtin
Account Operators	TheFirm.com/Builtin

Managers; Print Operators

Figure 8-7 Adding an account to the Managers and Print Operators groups

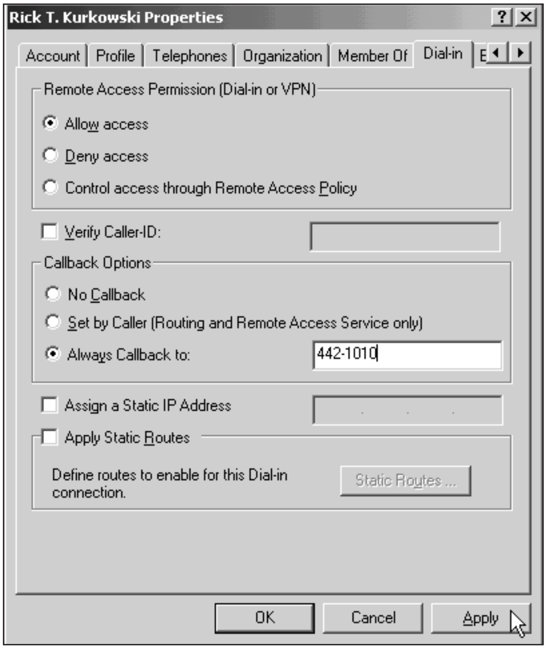
- *Dial-in:* Permits you to control remote access to the domain or to an intranet, for example from dial-in modems. Remote access can be allowed, denied, or controlled through a policy (see Figure 8-8). To enable an account holder to access the server or domain from a home computer or while on the road, click Allow access. Also, set up **callback security** options for dial-in access so a server's modems can call back the accessing workstation after the initial request to log on is received. This enables the server to verify that the call is from a known location. The callback can be set from the workstation's modem or from a prearranged number used by the server. There are also options to verify by caller ID, to configure a static IP address for the remote computer, and to enable static routing. (Dial-in security is presented in detail in Chapter 12.)

- *Environment:* Enables you to configure the startup environment for clients that access Windows 2000 Server using terminal services, which means that the client simulates a terminal instead of acting as an independent workstation with its own CPU. The options include the ability to specify that a startup program be run and that client devices, such as disk drives and printers, be connected.

- *Sessions:* Used to configure session parameters for a client using terminal services, such as a session time limit, a limit on how long a session can be idle, what to do when a connection is broken, and how to reconnect.

- *Remote Control:* Enables you to set up remote control parameters for a client that uses terminal services. The remote control capability enables you to view and manipulate the client session while it is active, in order to troubleshoot problems.

- *Terminal Services Profile:* Used to set up a user profile for a client that uses terminal services.



Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

○ No Callback

○ Set by Caller (Routing and Remote Access Service only)

● Always Callback to: 442-1010

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Figure 8-8 Configuring remote access

Creating an OU and Delegating Account Management

When you need to establish a group of accounts that have similar characteristics, for example for members of a particular department such as the payroll office, you have the option to create an OU (organizational unit) and place accounts in that container (but only if the Active Directory is installed). In this example, the OU might be called Payroll. You create the OU by clicking the domain in the left pane of the Active Directory Users and Computers console tree, clicking the *Create a new organizational unit in the current container* button on the button bar, entering the name of the OU (Payroll), and clicking OK. To create accounts in the OU, double-click the Payroll OU to open it in the console tree under the domain name, and click the *Create a new user in the current container* button on the button bar. Users are created as presented in the last section.

You also have the option to delegate management of accounts in the Payroll OU to a user or group. For example, you might delegate authority for creating new accounts in the Payroll Department to the payroll director. The steps that you use to delegate authority are as follows:

1. Right-click the OU, such as Payroll in our example, and click Delegate control.
2. When the Delegation of Control Wizard starts, click Next.
3. Click the Add button, double-click the user, group, or computer to which you want to delegate control. Add all of the users and groups that are appropriate. Click OK and click Next.

4. Make sure *Delegate the following common tasks* is selected, and then click the tasks that you are delegating, such as *Create, delete and manage user accounts* and *Reset passwords on user accounts*. Click Next. If instead you click *Create a custom task to delegate*, then you can customize how you want to delegate tasks by completing two additional dialog boxes for customizing object types and permissions. Click Next after completing each additional dialog box. The common delegated tasks are presented in Table 8-2.
5. Click Finish.

Table 8-2 Delegation of Control Options

Task	Description
Create, delete, and manage user accounts	Ability to fully set up and manage accounts
Reset passwords on user accounts	Ability to reset a member user's account password, should that user forget his or her password
Read all user information	Ability to access any information owned by the selected user accounts
Create, delete, and manage groups	Ability to set up and delete groups and modify group properties
Modify the membership of a group	Ability to add and delete members in a group
Manage Group Policy links	Ability to change the specified group policies or elements of a group policy

Account Maintenance

There are many options for maintaining an account after it has been created. One option is to double-click the account and change properties on the appropriate tabs, which has already been discussed. Also, there are maintenance shortcuts that you can access by right-clicking the account. The following sections describe shortcuts to maintenance activities that you are likely to perform frequently. If you have the Active Directory installed, these maintenance operations are performed using the Active Directory Users and Computers MMC snap-in; if the Active Directory is not installed, use the Local Users and Groups snap-in. If you are using the Active Directory Users and Computers snap-in, you will find accounts by locating the domain and then locating the Users or OU container under that domain. If there are many Active Directory OUs and levels of OUs, then you will need to look in each level until you find the account. Accounts in the Local Users and Groups snap-in are simply found under Users. If there are many OUs and levels of OUs, you can use the Find utility to locate an account. To use this utility:

1. Right-click the domain.
2. Click Find.

3. Enter the username (such as SGonzales), the account display name (such as Sarah Gonzales), or a portion of one of these (such as Gonzales).
4. Click Find Now.

Disabling, Enabling, and Renaming Accounts

When a user takes a leave of absence, for example for family leave, you have the option to disable his or her account.Your organization may also have the practice of disabling accounts when someone leaves and later renaming the account for that person's replacement (which is easier than deleting the account and creating a new one).To disable an account, right-click it and click Disable Account. Click OK when you see the informational dialog box that verifies you have disabled the account.The account icon will have an "x" in a red circle to show that it is disabled (see the Guest account shown earlier in Figure 8-2). No one can access the account until you enable it. To enable an account when the Active Directory is installed, right-click the account, click Enable Account, and click OK. If the Active Directory is not installed, right-click the account, click Properties, click the General tab, click Account is disabled, and click OK.

Renaming an account is nearly as easy as disabling and enabling one.To rename an account:

1. Right-click the account in the Active Directory Users and Computers snap-in and click Rename if the Active Directory is installed; if the Active Directory is not installed, right-click the account in the Local Users and Groups snap-in and click Rename.
2. In the highlighted box, enter the new name as you will see it in the Active Directory Users and Computers snap-in, for example renaming an account called Jason Brown to one called Sarah Gonzales.
3. Press Enter if the Active Directory is installed; if it is not installed, press Enter twice and provide the new name information in the General tab.
4. Complete the Rename User dialog box by entering the new full name, first name, last name, display name, user logon name, domain, and pre-Windows-2000 logon name (which is usually the same as the logon name and is used for naming via the UNC naming format).
5. Click OK.The renamed account will retain the same account properties, including access privileges and group memberships, as in the original account.

(Try Hands-on Project 8-2 to practice renaming and disabling an account.)

Moving an Account

When an employee moves from one department to another, for example from the payroll department to the budget office, you may need to move the account from one container to another—between OUs, for example.To move an account, right-click it and click Move. In the Move dialog box, double-click the domain to which to move the account, and the container, such as an OU or the Users container. Click OK and the account is moved by the Active Directory.

Deleting an Account

You can delete an account by right-clicking that account, clicking Delete, and clicking Yes to confirm the deletion (try Hands-on Project 8-2). When you delete an account, its globally unique identifier (GUID, see Chapter 4) is also deleted and will not be reused even if you create another account using the same name.

Resetting a Password

Sometimes users change their passwords or go several weeks without logging on—and forget their passwords. You do not have the option to look up a password, but you can reset it for the user. To reset a password, right-click the account, click Reset Password (or Set Password if the Active Directory is not installed), enter a new password, and confirm the password. When the Active Directory is installed, there is also a box that enables you to require that the user change his or her password as soon as he or she logs on. Checking the box enables you to force the user to change the password you set, so that you will not know the new password, which is often a requirement of auditors who scrutinize networks that handle financial information.

Account Auditing

Once accounts are set up, you can specify account **auditing** to track activity associated with those accounts. For example, some organizations need to track security changes to accounts, while others want to track failed logon attempts. In a college setting, security changes might be tracked on part-time students who work in sensitive administrative areas such as the registrar's office. Many server administrators track failed logon attempts for the Administrator account, to be sure an intruder is not attempting to access the server. Accounts that access an organization's financial information often are routinely audited to protect their users as well as the information they access. The events that can be audited are as follows:

- Logon and logoff activity
- Account modifications via management tools
- Accesses to files and objects (for files and folders set up to be audited)

Each listed activity is audited in terms of the success or failure of the event. For example, if logon attempts are audited, a record is made each time someone logs on to an account successfully or unsuccessfully.

CAUTION

Use auditing sparingly. Each audited event causes a record to be made in the Security event log. For example, if you audit all logon attempts of 200 domain accounts, the server log will quickly become loaded down just from auditing events and have fewer resources to perform other work.

Account auditing is configured as a group policy. For example, if your organization is required to set up account auditing for all accounts in a domain, first make sure that the default domain policy is set up as an MMC snap-in. In the MMC tree in the left pane, double-click Default

Domain Policy, double-click Computer Configuration, double-click Windows Settings, double-click Security Settings, double-click Local Policies, and click Audit Policy. In the right pane, double-click the policy you want to set up, such as Audit Account Logon events.

CUSTOMIZING CLIENT ACCESS WITH PROFILES

Client access to Windows 2000 Server can be customized through user and roaming profiles. A **local user profile** is automatically created at the local computer when you log on to an account for the first time, and the profile can be modified to consist of desktop settings that are customized for one or more clients who log on locally to the server. For example, if there are two server administrators and two backup operators who primarily run backups, you might want to create one profile for the administrators and a different one for the backup operators. That can be useful if each type of account needs to have certain program icons, startup programs, or some other prearranged desktop settings. Also, a user profile can be set up so it is downloaded to the client workstation each time a specific account is logged on. This is a **roaming profile**, which enables a user to start off with the same desktop setup, no matter which computer she or he uses in the office.

Note

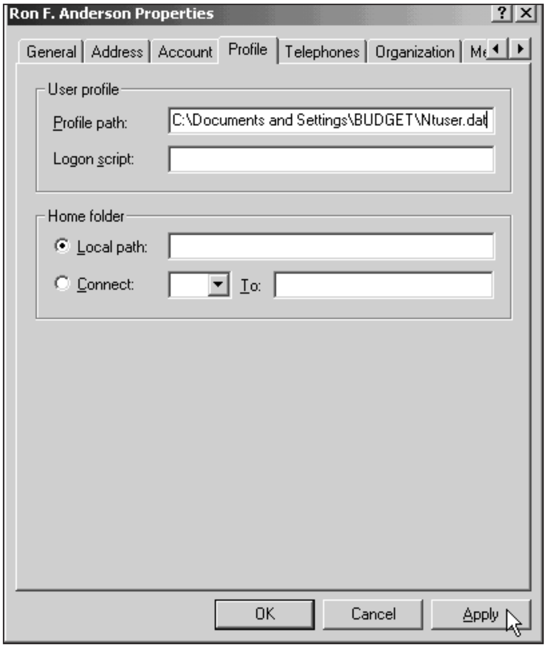
Profiles are used in Microsoft operating systems to provide a consistent working environment for one or more users. A local user profile is a particular desktop setup that always starts in the same way and is stored on the local computer. A roaming profile is a desktop setup that starts in the same way from any computer used to access an account, including remote connections from home or on the road. A **hardware profile** provides a consistent hardware setup for a user at the server console, such as keyboard, display type, and other hardware components. Different hardware profiles are not used much in Windows 2000 Server, but are used more commonly in Windows 2000 Professional to facilitate portable computing.

In some circumstances, you need to set up profiles so that certain users cannot change their profiles. This is done by creating a **mandatory user profile** in which the user does not have permission to update the folder containing his or her profile. A mandatory user profile overrides the user' s locally stored profile if it has been changed from the version stored on the server. To make a server profile (either local or roaming) mandatory, rename the user's Ntuser.dat file in the user's profile folder as Ntuser.man. The user's profile folder is found in \Documents and Settings*username*.

TIP

If you do not assign a profile to a user's account, a default user profile is loaded by the server when the user logs on. Located in the \Documents and Settings\Default User folder, the default user profile is also loaded automatically when an account's assigned profile cannot be accessed. However, if a mandatory profile cannot be accessed for some reason, the user will not be able to log on because the default profile is not loaded in this situation.

An easy way to set up a profile is to first set up a generic account on the server or use the Guest account as a model with the desired desktop configuration, including desktop icons, shortcut folders, and programs in the Startup folder to start when the client workstation starts. Then copy the model to the \Documents and Settings\Default User folder, naming it Ntuser.dat. This step makes that profile the default for new users. You can also create a profile to use as a roaming profile for specific users. To create the roaming profile, set up a generic account and customize its desktop. For example, you might create an account called BUDGET for users in the budget office and customize its desktop. After you create that account, set up those users to access that profile by opening the Profile tab in each user's account properties and entering the path to that profile, as in Figure 8-9. You can also use the System icon (User Profiles tab) in the Control Panel to copy profiles from one account folder to another (try Hands-on Project 8-3).



Profile path: C:\Documents and Settings\BUDGET\Ntuser.dat

● Local path:

○ Connect:

Figure 8-9 Setting a roaming profile in an account's properties

CONFIGURING CLIENT OPERATING SYSTEMS

After setting up accounts, it is also necessary to configure client computers to access those accounts. Many types of client operating systems can connect to Windows 2000 Server, including:

- MS-DOS
- Windows 3.1
- Windows for Workgroups
- Windows NT Workstation and Server
- Windows 2000 Professional
- Macintosh

- Windows 95
- Windows 98
- UNIX
- NetWare clients and servers

In general, when you configure a client operating system to connect, it is necessary to provide a way to identify the workstation to the network, by providing a name for the workstation and the domain it will join. Next, it is necessary to configure the protocol or protocols used to connect, such as TCP/IP, and to bind protocols to the NIC. Hands-on Projects 8-4, 8-5, and 8-6 give you practice in configuring the client operating systems you are most likely to encounter: Windows 3.11, Windows 95 and 98, and Windows NT 4.0. (Windows 2000 Professional is not included because you learned how to configure Windows 2000 operating systems in Chapter 6.)

Installing Active Directory Support for Non-Windows-2000 Clients

Microsoft offers the **Directory Service Client** (**DSClient**) software for Windows 95 and higher clients that connect to Windows 2000 Server. Directory Service Client does not provide the complete Active Directory Client features that are built into the Windows 2000 operating systems, but it does enable non-Windows-2000 clients to profit from two important capabilities: (1) the ability to use Kerberos authentication security, and (2) the ability to view information published in the Windows 2000 Active Directory, such as all network printers. To use DSClient, the client must have Internet Explorer 4.0 or higher and 10 MB of free disk space.

The DSClient program, Dsclient.exe, is located on the Windows 2000 Server CD-ROM in the folder \Clients\Win9x. To install the Directory Service Client software on a Windows 95 or Windows 98 client:

1. Copy DSClient.exe to a shared folder, such as one called DSClient, on a Windows 2000 server so that clients can access it over the network.
2. Log on to the domain from the client, such as Windows 98. Double-click Network Neighborhood on the client's desktop, find the host Windows 2000 server, double-click the server, and then double-click the shared folder containing DSClient.exe.
3. Double-click the DSClient.exe file and wait for the installation software components to be extracted into the client operating system.
4. The Directory Service Client Setup Wizard starts automatically. Click Next.
5. Click Next so that the Wizard can detect the system setup and copy the Directory Service Client files.
6. Click Finish and then click Yes to restart the client computer.

DSClient installs new features at the client, such as the ability to search the Active Directory for printers, even if the client does not know the specific name of a printer. To search for a printer using Windows 98 for example, click Start, point to Find, and click Printers (Printers is a new option added by the Directory Service Client).

TIP

Windows 95 also does not include the Distributed File System (Dfs; see Chapter 10) client software, while Windows 98 and Windows NT 4.0 do have the Dfs client software already installed. *When you install DSClient in Windows 95, it installs the Dfs client software along with the Directory Service Client software*. Dfs enables you to set up shared folders so that the client only needs to query the Dfs services for a hierarchy of shared folder locations, without first knowing which server contains the folder.

Setting Up Client Desktops Using Group Policy and Security Policy

In Windows NT 4.0 the desktop and other options viewed by clients can be customized by using the System Policy Editor as well as through user profiles. Windows 2000 Server uses group policies in place of the system policies, and system policies in Windows NT Server 4.0 are not migrated when you convert to Windows 2000 Server. However, it is possible to set up system polices in Windows 2000 Server that are compatible with Windows NT Server 4.0, if you have a domain with a mix of Windows NT and Windows 2000 servers, for instance.

Windows 2000 Server is installed with a default administrative template in group policies. For example, the default domain policy called System.adm can be configured to set up a consistent desktop in Windows 2000 Professional clients. Table 8-3 shows the administrative templates that are included with Windows 2000 Server to control client settings using group policy and using system policies.

TIP

When you have an environment that contains non-Windows-2000 clients, you can also use Windows NT Server 4.0 compatible system policies that you set up using the Poledit.exe tool, located in the Windows 2000 Server \Winnt folder. This tool starts the System Policy Editor, which works in a similar manner to the equivalent tool in Windows NT Server 4.0. It is recommended that you implement group policies instead of system policies in Windows 2000, to take full advantage of the Active Directory and lower TCO.

Table 8-3 Administrative Templates Included with Windows 2000

Template	Purpose	Tool Used to Configure
Common.adm	Managing desktop settings that are common to Windows 95, 98, and NT	Poledit.exe
Ientres.adm	Default for managing Internet Explorer in Windows 2000 Professional clients	Group Policy snap-in or edit group policy by using the Active Directory Users and Computers tool
System.adm	Default for managing Windows 2000 Professional clients	Group Policy snap-in or edit group policy by using the Active Directory Users and Computers tool
Windows.adm	Managing Windows 95 and 98 clients	Poledit.exe
Winnt.adm	Managing Windows NT 4.0 clients	Poledit.exe

The Windows 2000 Server group policy settings offer a wide range of ways to configure the Windows 2000 Professional client desktop. Table 8-4 presents the components that you can manage using the default template, System.adm.

Table 8-4 Group Policy Components for Windows 2000 Clients

Component	Description
Windows Components	Controls access to installed software such as NetMeeting, Internet Explorer, MMC, Task Scheduler, and Windows Installer
Start Menu & Taskbar	Controls the ability to configure the Start menu and Taskbar, the ability to access program groups from the Start menu, and the ability to use Start menu options, including Run, Search, Settings, and Documents
Desktop	Controls access to desktop functions, including the icons for My Network Places, Internet Explorer, and the ability to configure the Active Desktop
Control Panel	Controls access to Control Panel functions such as Add/Remove Programs, Display, Printers, and Regional Settings, plus the ability to disable the Control Panel altogether
Network	Controls access to offline files and the ability to configure network access via Network and Dial-up Connections
System	Controls access to Logon/Logoff capabilities, scripts, Task Manager functions, Change Password, and other system functions

To configure Windows 2000 Professional client desktops in the default domain policy, for example:

1. Open the Active Directory Users and Computers tool.
2. Right-click the domain you want to configure, and click Properties.
3. Click the Group Policy tab.
4. Click Default Domain Policy and click Edit.
5. Double-click User Configuration and double-click Administrative Templates. (Keep in mind that System.adm is already installed by default.)
6. Double-click any of the component folders that you want to configure, as described in Table 8-4, such as Start Menu & Taskbar.
7. Double-click each of the entities that you want to configure, such as *remove common program groups from Start Menu*.

Using Remote Installation Services

Remote Installation Services (**RIS**) enable you to install Windows 2000 Professional on client computers in environments that use the Active Directory. RIS can also be used to create boot disks from which to start a remote Windows 2000 Professional installation. RIS is one of the Windows 2000 Server options that enable you to reduce the cost (lower TCO, see Chapter 1) of managing a Windows 2000 network. When you install Windows 2000 Professional clients from a RIS server, you start by taking these steps:

1. Purchase licenses for the clients you wish to install.
2. Make sure the network that uses the Active Directory already has DHCP and DNS servers (see Chapters 3 and 13).
3. Install RIS on the Windows 2000 server that will become the RIS server.
4. Create a Windows 2000 Professional operating system image that will be copied to client computers. The image can be created from a Windows 2000 Professional CD-ROM or from an existing client running Windows 2000 Professional.
5. Create user accounts for the client computer users who will install Windows 2000 Professional.

Note

Windows 2000 Professional is the only operating system that can be installed from a RIS server. This is different from Windows NT Server 4.0, which enables you to use the Network Client Administrator to remotely install MS-DOS, Windows 3.11, Windows 95, and Windows NT from a server. Unlike Windows 2000 Professional, none of these operating systems enables you to take full advantage of the lower TCO capabilities of Windows 2000 environments.

The client computer hardware for the RIS installation only needs to meet or exceed the minimum hardware requirements for Windows 2000 Professional, and does not have to match the hardware configuration of the RIS server. When you install Windows 2000 Professional on the client, the installation process uses Plug and Play to detect the unique hardware on the client, beginning with the NIC.

RIS uses an unattended answer file (a .sif image file) that you can customize for Windows 2000 Professional installations, for example to specify which file system to use. Also, if you are installing Windows 2000 Professional onto a client that already has a previously purchased copy of Windows 2000 Professional installed, you will need to modify the answer file for that installation so that it includes the product identification number of the retail version (see Chapter 5 for more information about the contents and syntax of an answer file). The product identification number is the key code that is located on the back of the CD-ROM jewel case. The answer file is located in the folder: \\Remoteinstall\Setup\language [such as English]\Images\Win2000.pro\I386\Templates\Ristndrd.sif. When you modify the Ristndrd.sif answer file to include the product ID, use the following syntax under the [Userdata] section of the file:

```
ProductID = "nnnnn-nnn-nnnnnnn-nnnnn"
```

Plan to install RIS on a Windows 2000 server during your system maintenance time or when no users are logged on to the server, because it is necessary to reboot after the installation. To set up a Windows 2000 server as a RIS server:

1. Click Start, point to Settings, and click Control Panel.
2. Double-click Add/Remove Programs.

3. Click Add/Remove Windows Components.
4. Scroll the Components box until you find Remote Installation Services, and then check the box for that option. Notice the required disk space and total disk space available report at the bottom of the Windows Components Wizard dialog box, and make sure you have enough disk space before you continue.
5. Insert the Windows 2000 Server CD-ROM and click Next. (Provide the path to the \I386 folder on the CD-ROM, if requested.) Click Finish after all components are installed.
6. Click Yes to reboot the computer, first making sure that no one is logged on; or click No but plan to reboot the computer as soon as there is an opportunity to have all users logged off.

> TIP
>
> If the Active Directory is installed and there are DHCP and DNS servers on the network, you can configure the DHCP server to authorize only specific servers to provide RIS installations. This is a security feature that enables you to prevent unauthorized replication of Windows 2000 Professional and to limit the possibility of viruses. You authorize a RIS server through the DHCP MMC snap-in via the console Action menu, *Manage authorized servers* option.

Configuring RIS

After RIS is installed, you need to configure the services. For example, to configure RIS in a situation in which you use a Windows 2000 Professional CD-ROM for the image files (instead of a live Windows 2000 Professional workstation):

1. Open the Add/Remove Programs icon in the Control Panel, if it is not already open.
2. Notice that the *Set up services* box in the middle of the screen shows that you still need to configure RIS. Click the Configure button under Configure Remote Installation Services. The Remote Installation Services Setup Wizard starts. Click Next.
3. Specify the location for the folders used by RIS, such as D:\Remoteinstall. Make sure that you use a drive other than the one that holds the Windows 2000 Server operating system files (the \Winnt folder) and click Next.
4. Select whether or not to enable the option to have RIS immediately support client computers, and click Next.
5. Specify the path to the Windows 2000 Professional CD-ROM that contains the installation files, and click Next.
6. Enter a name for the folder that is to contain the Windows 2000 Professional installation files, such as Win2000.pro, and click Next.
7. Enter the "friendly" description (for users) of the installation image files, such as Microsoft Windows 2000 Professional. Also, enter help text that the installer will

see, such as, "Automatically installs Windows 2000 Professional without prompting the user for input," which is the default text. Click Next.

8. Verify your installation selections and click Finish (or click Back to reconfigure a selection). The Wizard creates the installation folders, copies installation files, creates the unattended answer file, and completes setting up and starting RIS.
9. Click Done.

You can modify the RIS configuration and set up advanced RIS capabilities by accessing the RIS server in the Active Directory Users and Computers tool. To modify these settings, open Active Directory Users and Computers and double-click the domain that contains the RIS server. Next, double-click Domain Controllers, if the server is a DC, or click Computers if it is a member computer. Right-click the RIS server, click Properties, and click the Remote Install tab. The tab contains three buttons:

- *Verify Server:* Verify that the installation files are fully intact.
- *Show Clients:* View RIS clients that are currently connected to the server.
- *Advanced Settings:* Set up a RIS client computer naming convention, specify the directory service location, and add, remove, or modify images.

On a network in which there is a computer naming convention or in which there are naming conventions that vary by group, you may want to establish RIS computer naming conventions by domain or by OU. For example, in one domain the computer names may be set up to match each user's account name, while in another domain the computer names may be set up to enable customized naming. In another example, computer names may vary by OU so that those in the Customer Service OU are set up as the user's first initial followed by the last name and those in the Marketing OU are set up as the user's first name followed by her or his last initial. Hands-on Project 8-7 shows how to configure computer naming by Active Directory location.

Using RIS to Install Windows 2000 Professional on the Client Computer

The Windows 2000 Professional operating system files are installed on the client in one of two ways: by purchasing a client computer that has a Windows 2000 compatible remote-boot-enabled ROM or by creating a remote boot disk. Both support what Microsoft calls the **Preboot eXecution Environment** (**PXE**). PXE works with DHCP when the prospective client first boots and enables the client to request an IP address and a network connection to the RIS server. At the same time, the client is registered in the Active Directory with a computer name and a unique GUID (see Chapter 4). The steps that you use to create a remote boot disk are:

1. Insert a blank formatted floppy disk in the RIS server or in a Windows 2000 server or workstation that you can use to access the RIS server through the network.
2. Click Start, click Run, and enter the UNC path to the Rbfg.exe file, for example: D:\Remoteinstall\Admin\I386\Rbfg.exe. (If you run the file from another

computer used to access the RIS server, such as one running Windows 2000 Professional, enter the UNC path instead and make sure that the Remote install folder on the RIS server is shared.) Click OK.

3. Specify the drive on which to copy the files, such as drive A. There is an Adapter List button that enables you to check the adapters supported by the PXE process and Plug and Play detection at the client computer.
4. Click Create Disk.
5. Click Yes if you want to create another boot disk, or click No.
6. Click Close to exit the Windows 2000 Remote Boot Disk Generator.

CAUTION

The client should have a NIC that is listed on the Windows 2000 Professional HCL and that is supported by RIS. Also, if you experience boot problems, set up the computer's BIOS to use the NIC as the device from which to boot first.

When you boot the client computer using the remote-boot-enabled ROM or the remote boot disk, PXE launches the Client Installation Wizard. After the Wizard starts, press Enter and then provide the username, password, and domain name. Select the specific installation option from those listed in Table 8-5.

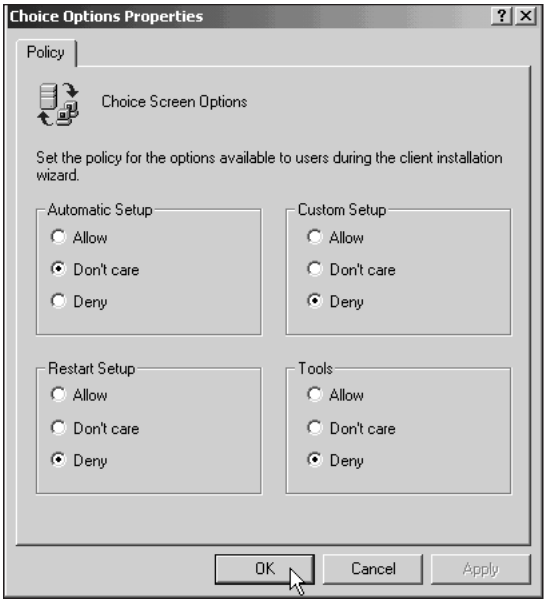
Table 8-5 Client Installation Wizard Options

Option	Description
Automatic Setup	Uses the unattended answer file to perform a complete Windows 2000 Professional installation without interactive input from the user
Custom Setup	Uses the unattended answer file to perform a Windows 2000 Professional installation, but enables the user to specify the computer name and location in the Active Directory
Restart	Enables the user to restart an installation that was previously interrupted (due to a power outage, for example, or that did not complete because of an installation problem)
Maintenance and Troubleshooting	Enables the user to troubleshoot an installation by using tools available through the Client Installation Wizard

Using Group Policies to Create Installation Groups

You can use group policies to create different installation options for different groups or containers, for example for different OUs or different domains. Before you link different installation options with different groups, first make sure that a group policy is in place for each container, and then modify the group policy. To associate a particular set of installation options with a container object:

1. Start the Active Directory Users and Computers tool.
2. Right-click the container you want to associate with particular RIS installation options, for example an OU or domain, and click Properties.
3. Click the Group Policy tab, click the group policy you want to modify under Group Policy Object Links, and click the Edit button.
4. In the left pane, click Windows Settings, which is located under User Configuration in the tree displayed for the group policy.
5. In the right pane, double-click Remote Installation Services.
6. In the right pane, double-click Choice Options.
7. Specify the type of user access for Automatic Setup, Custom Setup, Restart Setup, and Tools (see Figure 8-10).



Choice Options Properties

Policy

Choice Screen Options

Set the policy for the options available to users during the client installation wizard.

Automatic Setup
○ Allow
● Don't care
○ Deny

Custom Setup
○ Allow
○ Don't care
● Deny

Restart Setup
○ Allow
○ Don't care
● Deny

Tools
○ Allow
○ Don't care
● Deny

Figure 8-10 Setting RIS installation options through group policy

As Figure 8-10 shows, the policy options are Allow, Don't care, and Deny. Allow means that the designated capability can be used by client accounts that are defined in the container. Don't care is the default and means that the policy that applies to the parent container, such as the domain, applies to the current container, such as an OU in that domain. Deny means that the capability is not available to the group of users in the container.

Using RIS Troubleshooting Tools

Some third-party vendors offer troubleshooting and maintenance tools that can be used by administrators and users via the RIS server. A tool is installed by following the particular vendor's instructions. After tools are installed, you can view them by opening Active Directory Users and Computers, right-clicking the RIS server in the tree, clicking Properties, clicking the Remote Install tab, clicking the Advanced Settings button, and clicking the Tools tab. On the Tools tab you have three options. The Remove button is used to remove a particular tool from the unattended answer file, so that tool is not available to the user. The Properties button enables you to view the tool's properties and to modify the description of the tool that users will see. The Refresh button simply redisplays the RIS tool listing on the Tools tab.

Chapter Summary

- Preparing a Windows 2000 server and domain for user access involves two essential steps: configuring user accounts and configuring individual client computers to access the network. Before you configure accounts, establish guidelines for account names. You may need to work with different groups, departments, or management bodies to develop naming guidelines that correspond to your organization's needs. Also, consult with members of your organization prior to establishing account security policies. Account security policies enable you to protect data and network resources through establishing password restrictions, account lockout security, and Kerberos security.

- After you have established naming guidelines and set up account policies, create accounts by using the Local Users and Groups snap-in for a standalone server that is not part of a domain, or by using the Active Directory Users and Computers snap-in when the Active Directory is in use. Account properties can be set up to provide information about an account holder that includes telephone numbers, address information, and Web page information. You can also control how the account accesses the domain, such as by limiting access via a specific computer. Other ways to manage access include creating profiles, configuring group policies, and setting up system policies. Client computers must each be configured to access the network so that they can log on to accounts. The configuration steps include installing and configuring protocols for operating systems such as Windows 3.11, Windows 95/98, Windows NT, and others.

- Remote Installation Services (RIS) is an option that enables you to install Windows 2000 Professional on multiple clients from a RIS server. RIS can greatly reduce the TCO of network management by automating the setup of clients.

In the next chapter, you learn how to manage server folders and groups, and you learn more about security options.

KEY TERMS

account lockout — A security measure that prohibits logging on to a Windows 2000 server account after a specified number of unsuccessful attempts.

auditing — Tracking the success or failure of events by recording selected types of events in an event log of a server or a workstation.

callback security — Used for remote communications verification; the remote server calls back the accessing workstation to verify that the access is from an authorized telephone number.

Directory Service Client (**DSClient**) — Microsoft software for Windows 95 and higher clients that connect to Windows 2000 Server that enables non-Windows-2000 clients to use Kerberos authentication security and to view information published in the Windows 2000 Active Directory, such as all network printers.

hardware profile — A consistent setup of hardware components associated with one or more user accounts.

local user profile — A desktop setup that is associated with one or more accounts to determine what startup programs are used, additional desktop icons, and other customizations. A user profile is local to the computer in which it is stored.

logon script — A file that contains a series of commands to run each time a user logs on to his or her account, such as a command to map a home drive.

mandatory user profile — A user profile set up by the server administrator that is loaded from the server to the client each time the user logs on; changes that the user makes to the profile are not saved.

Preboot eXecution Environment (**PXE**) — Services on a Windows 2000 remote-boot-enabled ROM or a remote boot disk that enable a prospective client to obtain an IP address and to connect to a RIS server in order to install Windows 2000 Professional.

primary group — A group designation used when setting up a Windows 2000 server account for workstations running Macintosh or POSIX. Windows 2000 Server requires that these systems be members of a global security group.

Remote Installation Services (**RIS**) — Services installed on a Windows 2000 Server that enable you to remotely install Windows 2000 Professional on one or more client computers.

roaming profile — Desktop settings that are associated with an account so that the same settings are employed no matter which computer is used to access the account (the profile is downloaded to the client).

service ticket — A Kerberos security key that gives a client access to specific services on a server or in a domain for a designated period of time.

Universal Naming Convention (**UNC**) — A naming convention that designates network servers, computers, and shared resources. The format for a UNC name is \\Servername [or *Computername*]*Sharename**Folder**File*.

Windows NT LAN Manager (**NTLM**) — An authentication protocol used in Windows NT Server 3.5, or 3.51, and 4.0 that is retained in Windows 2000 Server for backward compatibility with clients that cannot support Kerberos, such as MS-DOS and Windows 3.1x.

REVIEW QUESTIONS

1. You are the server administrator in the IT department of a community college. The financial auditors have just visited the college and have written up a concern that the Administrator account on the Windows 2000 server used for accounting can be accessed from anywhere on campus and even through remote dial-up access. How can you tighten security?

   a. Limit on-campus access to the Administrator account to the computer in your office.

   b. Rename the Administrator account to match your name.

   c. Set up the Administrator account Dial-in properties to use callback security.

   d. all of the above

   e. only b and c

   f. only a and c

2. The financial auditors mentioned in Question 1 also want to disable access to the server over the weekend to all users but you and the Accounting Department. How can this be done?

   a. Limit the logon hours in the account properties for all accounts that should not have access over the weekend.

   b. Put the server in hibernate mode during the weekends, except by special arrangements for Accounting Department members who provide you with advance notice.

   c. Use the account auditing feature in Windows 2000 to limit who can access accounting folders over the weekend.

   d. There is no way to limit access to meet this request.

3. Which of the following are examples of password policies that can be set up in group policies?

   a. Require that a password must be entered in the reverse order in which it is spelled.

   b. Require a minimum password length.

   c. Require that a password contain only proper names.

   d. all of the above

   e. only a and b

   f. only b and c

4. Mary Balsam is your organization's chief information officer and has specialized security access to resources in the domain. She is retiring on Friday, and the new CIO starts the next Friday. What is the easiest way to handle Mary's departure and set up an account for the new CIO?

   a. Delete Mary's account at the end of Friday and set up a new account for the incoming CIO on the following Friday.

   b. Create a copy of Mary's account for the new CIO and then delete Mary's account.

c. Disable Mary's account at the end of Friday, and when the new CIO arrives, enable Mary's account and rename it for the new CIO.

d. Create a new account for the incoming CIO and move it to a new domain.

5. Which of the following are account policies that you can set up for a domain?

a. Kerberos

b. account lockout

c. password

d. all of the above

e. only a and b

f. only b and c

6. The board of directors for your organization wants the five department heads in the organization to set up and manage accounts for employees in each of their departments. How can you best help them accomplish this via the Active Directory?

a. Give each department head administrator privileges.

b. Create an OU for each department and delegate account management in each OU to the appropriate department head.

c. Create a domain for each department and make the department head administrator for her or his domain.

d. Show each department head how to take control of administrator privileges, because Windows 2000 Server requires this step in order to delegate these privileges.

7. Which of the following might be used in a logon script?

a. homepath

b. temppath

c. homedrive

d. all of the above

e. only a and b

f. only a and c

8. From where do you set an account to use a logon script?

a. account properties

b. account policies

c. Kerberos policies

d. domain setup properties

9. Which of the following clients would require an account in which a primary group is specified?

a. Windows 3.1

b. Windows 3.11

c. Macintosh

d. Windows 2000 Professional

10. Your organization requires that all Windows 2000 Professional users must use the same desktop setup and that there be an icon on the desktop that opens an inventory program. How can you set this up?

a. Associate a mandatory profile with each of these users' accounts.

b. Associate a local user profile with each of these users' accounts.

c. Make sure the properties in each account are set to log on from a specific computer in each employee's office.

d. There is no way to enforce use of the same desktop because users can configure and save any number of possibilities in Windows 2000 Professional.

11. As server administrator, how can you most easily make sure you do not know your users' passwords?

a. Make each user an account administrator so that users must create their own accounts.

b. When you set up an account, have the user come to your office at the same time and type in his or her password.

c. Delegate password authority to each user.

d. Check the box User must change password at next logon, when you create the account.

12. Which administrative template enables you to manage desktop settings for Windows 2000 Professional clients, and what tool do you use to set it up?

a. Winnt.adm using the Group Policy MMC snap-in

b. Common.adm using the Poledit.exe System Policy Editor

c. Windows.adm using the Poledit.exe System Policy Editor

d. System.adm using the Group Policy MMC snap-in

13. Ntuser.man is a:

a. logon script

b. mandatory profile

c. home folder

d. Administrator account profile

14. A Windows 2000 Server password can be up to ________________ characters in length.

a. 7

b. 10

c. 20

d. 64

15. Which of the following enables you to copy an existing profile to an account's setup folder in Windows 2000 Server?
    a. Control Panel System icon
    b. Control Panel Network icon
    c. Active Directory Users and Computers MMC snap-in
    d. Local Computers and Users MMC snap-in
16. You have set up a Windows 95 client to access a Windows 2000 Server domain called Buffalo. When you log on from that client using the account name and password for the account that you created in the Windows 2000 Active Directory, you still do not see the computer as part of the domain. What might be the problem?
    a. You did not specify the domain name in the Windows 95 network setup.
    b. You did not enter a computer name in the Windows 95 network setup.
    c. You did not set up NetBEUI as a protocol in Windows 95, and this protocol must be used along with TCP/IP for Windows 95 connectivity to Windows 2000 Server.
    d. All of the above might be problems.
    e. Only a and b might be problems.
    f. Only a and c might be problems.
17. Which of the following is(are) true about setting up accounts in Windows 2000 Server?
    a. Accounts must be set up only in the Users container under the domain when the Active Directory is implemented.
    b. Accounts must have a password that is at least five characters long.
    c. Accounts can be set up so that the user cannot change the password.
    d. all of the above
    e. only a and b
    f. only b and c
18. When Kerberos is enabled in the Active Directory on a network that has 225 users, four domain controllers, and a member server, which of the following are key distribution centers?
    a. each client
    b. each domain controller
    c. only the domain controller that is set up first on the network
    d. only the member server
19. Which of the following models is(are) used for naming conventions?
    a. user's first two initials and last name
    b. user's position name in an organization
    c. user's function in an organization
    d. all of the above

e. only a and c

f. only b and c

20. Which of the following characters can be in a Windows 2000 Server account password?

a. [

b. >

c. =

d. none of the above

e. only a and b

f. only b and c

21. Which of the following can you perform on the *Member Of* tab in the properties of an account?

a. adding the account to a group

b. specifying the domain in which the account belongs, when the Active Directory is implemented

c. providing telephone numbers associated with the account holder

d. all of the above

e. only a and b

f. only a and c

22. Your network is set up to enable users to install Windows 2000 Professional from a RIS server. However, your boss has heard that another department is considering the implementation of a RIS server, but that it is lax on obtaining licenses. He wants to know if you can centralize installations only from your server in the IT department, as a way to ensure proper licensing. What is your reply?

a. There is no way to prevent network users from installing Windows 2000 Professional from another department's RIS server.

b. You can configure the network's DNS server so that it does not contain the IP addresses of other departments' servers.

c. You can configure the network's Windows 2000 DHCP server so it only authorizes RIS installations from your RIS server.

d. As network administrator, you can alter the Registries of all other RIS servers so that user connections time out before completing a full Windows 2000 Professional installation.

23. The president of your company has just changed his password and forgotten it. How can you help as the server administrator?

a. Look up his password and give it to him.

b. Reset his password, require that he change it as soon as he logs on, and give him the password that you reset.

   c. Rename the president's account and give him the new password you set up in the process.

   d. Delete and recreate the president's account and give him the new password you set up in the process.

24. You want to enable users in the Shipping OU to use RIS to install Windows 2000 Professional using only the Automatic Setup option. Also, you want users in the Accounting OU to use only the Custom Setup. What feature of Windows 2000 Server enables you to customize these RIS installation options?

    a. Group Policy

    b. Security Manager

    c. RIS Manager

    d. Active Directory Domains and Trusts

25. During your lunch hour, you have been deleting, copying, and reworking several profiles stored in Windows 2000 Server. After lunch, one of the users calls to report that she cannot log on to the domain, but she had no problems logging on just before going to lunch. What problem would you suspect first?

    a. You made an illegal change in a local user profile.

    b. You accidentally deleted her mandatory profile.

    c. You accidentally deleted her roaming profile.

    d. You forgot to unlock her account after working on its profile.

HANDS-ON PROJECTS

Project 8-1

This project enables you to practice setting account password and lockout policies in Windows 2000 Server when the Active Directory is already installed. You have the option to view the policies as they are currently set and to change the policies (with permission from your instructor).

To view and configure the policies:

1. Click the **Start** button, click **Run**, enter **mmc**, and click **OK**. Maximize the console windows, if necessary. Click the **Console** menu and click **Add/Remove Snap-in**.
2. In the Add/Remove Snap-in dialog box, click **Add**, scroll to **Group Policy** and double-click it.
3. When the Select Group Policy Object Wizard starts, click the **Browse** button, double-click **Default Domain Policy**, and click **Finish**. Click **Close** and click **OK**. Double-click **Default Domain Policy** in the left pane, double-click **Computer Configuration**, double-click **Windows Settings**, and click **Security Settings**. What options are displayed in the right window pane? Record your observations in a lab journal or in a word-processed document.

4. In the right pane, double-click **Account Policies**. What options are now displayed in the right window pane? Record your observations.
5. Double-click **Password Policy**. Notice and record the options in the right pane.
6. If you have permission from your instructor to change parameters, double-click **Enforce password history**. Make sure **Define this policy setting** is checked, enter **10** in the Passwords remembered box, and click **OK**. Next, double-click **Minimum password length** and make sure **Define this policy setting** is checked. Enter **7** in the characters box on the Security Policy Setting dialog box, and click **OK**. Notice that your changes are now reflected in the right pane.
7. Click **Account Lockout Policy** in the tree displayed in the left pane. Record the options available in the right pane.
8. If you have permission from your instructor to change parameters, double-click **Account lockout threshold**. Make sure **Define this policy setting** is checked, enter **5** in the invalid logon attempts box, and click **OK**. What parameters are dependent on this one? Click **OK** to automatically set those parameters. (Note that this box may not be displayed, if the other lockout parameters are already set.) Record the changes that are now reflected in the right pane.
9. Close the MMC and click **No**, if asked whether to save your console settings.

Project 8-2

In this project, you practice setting up an account, configuring it, renaming it, disabling it, and then deleting it. The Active Directory must already be installed to perform this project.

To set up the account:

1. Click the **Start** button, click **Run,** enter **mmc**, and click **OK**. Maximize the console windows, if necessary. Click the **Console** menu and click **Add/Remove Snap-in**. Click **Add** and double-click **Active Directory Users and Computers**. Click **Close** and click **OK**. What is another way to access the Active Directory Users and Computers tool, beginning from the Start button?
2. In the left pane, double-click **Active Directory Users and Computers** and click the domain name that is displayed under it. Record in your lab journal or in a word-processed document the options that are now shown in the right pane.
3. Double-click **Users** in the right pane. Are there any accounts already created? What objects are shown along with the accounts?
4. Click the **Action** menu or right-click **Users** in the left pane, click **New** and click **User**.
5. Enter your first name in the First name box, enter your middle initial (no period), and enter your last name, with **test** appended to it, in the Last name box, for example: **Palmertest**. Enter your initials, with **test** appended to them, in the User logon name box, for example: **MPTest**. What options are automatically completed for you? Record these in your lab journal or in a word-processed document. Click **Next**.
6. Enter a password, such as **Palmertest**, and enter the password confirmation. Click the box to select **User must change password at next logon**. Click **Next**.
7. Verify the information you have entered and click **Finish**.

To configure the account:

1. In the right pane, double-click the account you just created.
2. Notice the tabs that are displayed for the account properties and record them in your lab journal or in a word-processed document. If you are using a smaller monitor, and depending on its resolution settings, you may need to use the back and forward arrows to access all of the tabs.
3. Click the **General** tab, if it is not already displayed, and enter a description of the account, such as **Test account**.
4. Click the **Account** tab.What information is already completed on this tab?
5. Click the **Logon Hours** button. In the Logon Hours dialog box, point to the first shaded box on the left under 12 for the bottom row, which is Saturday. Drag the pointer to the rightmost box for Saturday (which is also under 12). Click **Logon Denied** and click **OK**.
6. Click the tabs you have not yet viewed to find out what information can be configured through each one. Record your observations about each tab.
7. Click **Apply** and click **OK**.

To rename the account:

1. In the right pane, right-click the account you just created.
2. Click **Rename** and enter your first two initials, a space, and **Rename**, for example: **MJ Rename**.
3. Press **Enter**.
4. Enter your first two initials in the First name box and enter **Rename** in the Last name box. Enter your first two initials and **Rename** in the Display Name box, for example: **MJ Rename**.
5. Click **OK**. Notice the new name as it is displayed in the right pane.

To disable the account:

1. In the right pane, right-click the account you created and renamed.
2. Click **Disable Account** and click **OK**.
3. Notice the appearance of the account in the right pane. How has the appearance changed?

To delete the account:

1. In the right pane, right-click the account you created, renamed, and disabled (make sure you select the correct account).
2. Click **Delete** and click **Yes**.
3. What has happened to the account in the right pane?
4. Close the MMC and click **No**, if asked to save your console settings.

Project 8-3

In this hands-on activity you configure a default user profile for accounts created in Windows 2000 Server. (Your instructor may prefer that you use a different account than Guest as the account in which to configure the default user profile. Also, the Guest account or any other account that you use will need access to log on locally.)

To configure the default profile:

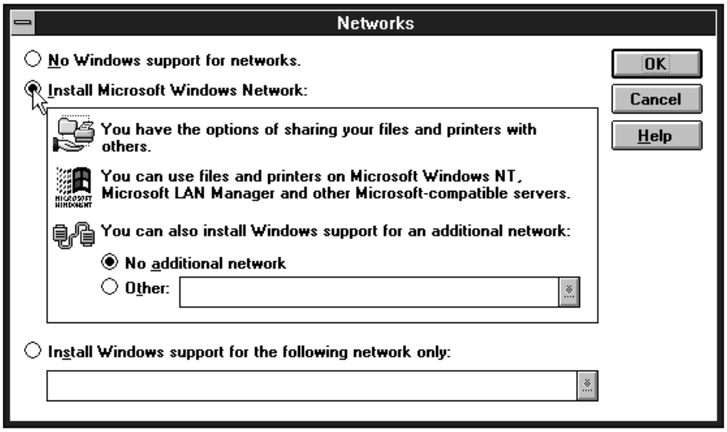
1. Log on to the Guest account.
2. Click **Start**, point to **Settings**, and click **Control Panel**.
3. Double-click the **Display** icon and click the **Background** tab. Click the **Pattern** button and select a pattern such as **Boxes** or **Diamonds**. Click **OK**. What are some other desktop settings that you might configure to set up the default user profile? Record your suggestions in a lab journal or a word-processed document.
4. Click **Apply** and click **OK**.
5. Click the **Start** button, click **Shutdown**, and scroll the Shut Down Windows dialog box to select **Log off Guest**. Click **OK**.
6. Press **Ctrl+Alt+Del** and log on to the Administrator account or another account with Administrator privileges.
7. Click **Start**, point to **Settings**, click **Control Panel**, and double-click the **System** icon.
8. Click the **User Profiles** tab, click the **Guest** account (or another account as specified by your instructor), and click the **Copy To** button.
9. Click the **Browse** button, locate and then click the **Default User** or **All Users** subfolder (depending on your setup) in the Documents and Settings folder, for example in **C:\Documents and Settings\Default User** or **C:\Documents and Settings\All User**. Click **OK** in the Browse for Folder dialog box.
10. Click **OK** in the Copy To dialog box and click **Yes** to confirm the copy (replace the current settings). Close the System Properties dialog box.
11. What happens to the display when you create a new account and log on to it? Record your findings. How can you make this a roaming profile?

Project 8-4

In this hands-on activity you configure Windows 3.11 to connect as a client to Windows 2000 Server.

To configure Windows 3.11:

1. After Windows 3.11 boots, open the **Main** program group in Program Manager.
2. Double-click the **Windows Setup** icon.
3. Click the **Option** menu and click **Change Network Settings**.
4. Click the **Networks** button in the Network Setup dialog box.
5. Click **Install Microsoft Windows Network:** and click **OK** (see Figure 8-11).


Networks

○ No Windows support for networks.

● Install Microsoft Windows Network:

You have the options of sharing your files and printers with others.

You can use files and printers on Microsoft Windows NT, Microsoft LAN Manager and other Microsoft-compatible servers.

You can also install Windows support for an additional network:

● No additional network

○ Other:

○ Install Windows support for the following network only:

Figure 8-11 Configuring Windows 3.11

6. Click the **Drivers** button in the Network Setup dialog box, and click the **Add Protocol** button. Notice the protocol options and record them in your lab journal or in a word-processed document.
7. If you have the TCP/IP protocol on a disk from Microsoft or from the NIC vendor, click **Unlisted or Updated Protocol**, click **OK**, insert the disk in drive A, and click **OK**. If you do not have the TCP/IP protocol available, click **Microsoft NetBEUI** and click **OK**.
8. Click **Close** in the Network Drivers dialog box.
9. Click **OK** in the Network Setup dialog box.
10. Click **OK** to modify the System.ini file.
11. Click **Restart Windows** to reboot with the new network settings.

CAUTION

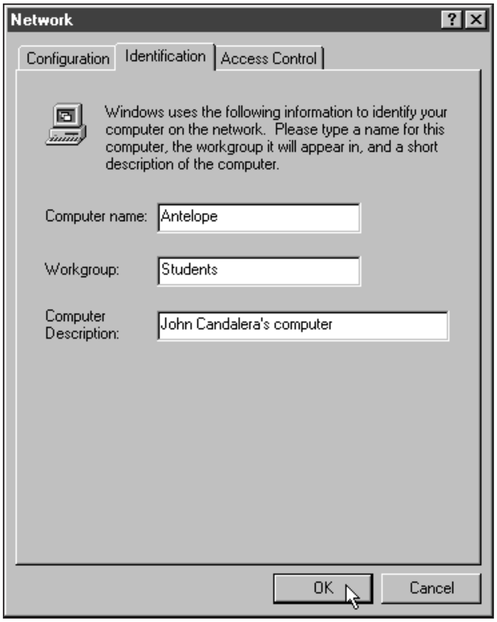
You can connect to a shared drive on Windows 2000 Server by opening File Manager from the Main program group and clicking the Connect Network Drive button. Another way to connect through File Manager is to click the Disk menu and click Connect Network Drive. The Connect Network Drive dialog box in Windows 3.11 contains an Always Browse option to enable you to browse domains, workgroups, and computers connected to the network. If this option is checked (which is the most likely condition), then Windows 3.11 may contend with Windows 2000 Server and Windows NT Server (and Windows NT Workstation and Windows 2000 Professional) computers as the Master Browser. A serious indication of this problem is seen when computers running Windows 95, Windows 98, Windows NT, and Windows 2000 experience problems in using Network Neighborhood or My Network Places, such as not seeing some or even all computers connected to the network. The solution is to modify the System.ini file in Windows 3.11 to have the line: MaintainServerList=no. As a Windows 2000 Server administrator, you can identify the contending Windows 3.11 system by checking the server System log for Master Browser contention (you will learn more about using the system log in Chapter 14).

Project 8-5

This project gives you an opportunity to practice setting up Windows 95 or Windows 98 as a client for Windows 2000 Server. Before you start, make sure that the computer you are setting up has a NIC already installed. Also, obtain a workgroup and domain name from your instructor and ask your instructor if the IP address is obtained automatically. If it is not, ask for an IP address and subnet mask (see Chapter 3).

To set up Windows 95 or 98 as a client:

1. Click **Start**, point to **Settings**, and click **Control Panel**.
2. Double-click the **Network** icon.
3. Click the **Identification** tab.
4. Enter a computer name, such as **Antelope** or your last and first name with 95 or 98 appended in the Computer name box, for example: **CandaleraJohn98**. Enter the workgroup name that you obtained from your instructor and enter a description, such as **John Candalera's computer** (see Figure 8-12).
5. Click the **Configuration** tab and click the **Add** button (see Figure 8-13).


Windows uses the following information to identify your computer on the network. Please type a name for this computer, the workgroup it will appear in, and a short description of the computer.

Computer name: Antelope

Workgroup: Students

Computer Description: John Candalera's computer

Figure 8-12 Configuring network identification in Windows 95 or 98

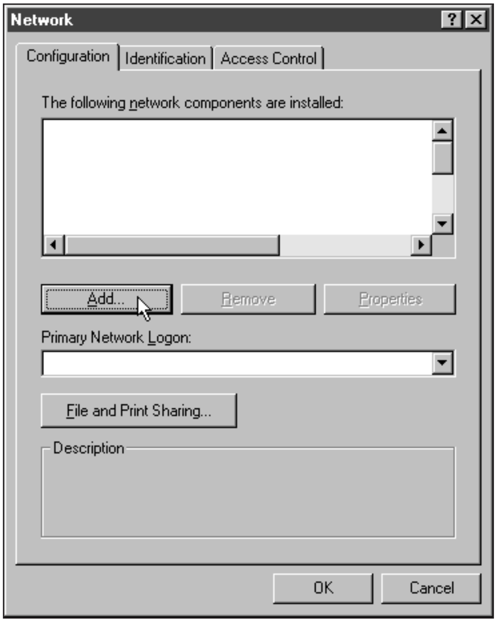


Figure 8-13 Configuring network connectivity in Windows 95 or 98

6. Double-click **Client** in the Select Network Component Type dialog box. What manufacturers are listed in the dialog box? Record your observations in your lab journal or in a word-processed document.
7. Click **Microsoft** in the Manufacturers: Select Network Clients box, click **Client for Microsoft Networks** in the Network Clients box, and click **OK**.
8. Back on the Configuration tab, click **Client for Microsoft Networks** and click the **Properties** button.
9. Click **Log on to Windows NT domain** and enter the domain name provided by your instructor in the Windows NT domain box. Also, click **Logon and restore network connections**. Click **OK**.
10. Again back on the Configuration tab, click the **Add** button on the Identification tab and double-click **Protocol**.
11. Click **Microsoft** in the Manufacturers box. Notice which protocols are available and record your observations. Click **TCP/IP** in the Network Protocols box and click **OK**.
12. On the Configuration tab, scroll to find **TCP/IP** → ***network card name***, click that selection, and click **Properties**. Record the tabs that you see displayed. Click the IP Address tab, if it is not automatically displayed.
13. If your network uses DHCP (see Chapter 3), click **Obtain an IP address automatically**. If, instead, your instructor gave you an IP address and subnet mask to use, click **Specify an IP address** and enter the IP address and subnet mask (remember to advance from field to field by pressing the period key).

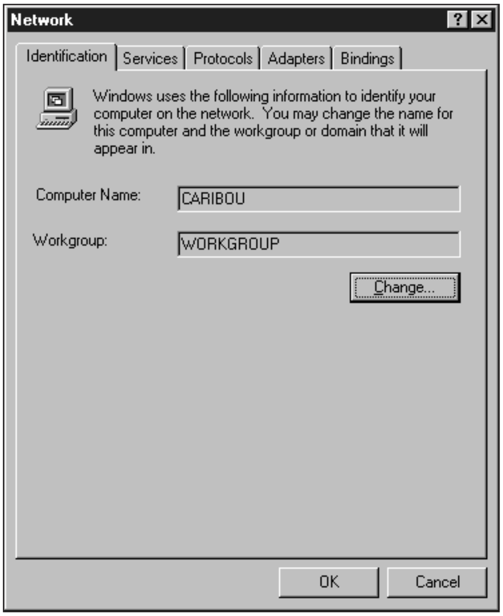
14. Click the **Bindings** tab and make sure that **Client for Microsoft Networks** is checked. If it is not, click that selection. Notice if there are other binding selections, and record your observation in your lab journal or in a word-processed document.
15. Click **OK** in the TCP/IP Properties dialog box.
16. Back on the Configuration tab, locate the computer's NIC in the scroll box, such as **3COM Fast EtherLink XL NIC**, and double-click it.
17. Click the Driver Type tab, if it is not already displayed. Make sure that the driver is **Enhanced mode (32 bit and 16 bit) NDIS driver**, and click that option if it is not already selected. Notice the other drivers that are available and record them in your lab journal or in a word-processed document.
18. Click **OK** in the Network dialog box and click **Yes** to restart the computer (make sure any open documents are saved first).

Project 8-6

This hands-on project gives you practice configuring Windows NT Workstation 4.0 as a Windows 2000 Server client. Before you start, make sure that the computer has an installed NIC and that you have an IP address and subnet mask, if these are not set through DHCP (consult your instructor). Also, you will need an account with Administrator privileges.

To configure Windows NT Workstation 4.0 as a client:

1. Log on to Windows NT 4.0 using your account and password.
2. Click **Start**, point to **Settings**, click **Control Panel**, and double-click the **Network** icon.
3. Click the **Identification** tab, if it is not already displayed (see Figure 8-14).
4. Click the **Change** button.
5. Enter the Computer Name, which is your last and first name concatenated along with NT, for example: **CandaleraJohnNT**, and click **OK** (Windows NT will check to make sure no other computer has the same name).
6. Click the **Change** button again. Click the **Domain** radio button.
7. Click **Create a Computer Account in the Domain** and enter the same account name and password that you used to log on to Windows NT Workstation. Note that this account must have been created earlier on the Windows 2000 Server domain controller. Click **OK** when you see the welcome dialog box.
8. Click the **Protocols** tab and click the **Add** button. Notice the protocols that you can install, and note them in your lab journal or in a word-processed document.
9. Click **TCP/IP protocol** and click **OK**.
10. Click **Yes** if your network uses DHCP, or click **No** if your instructor gave you an IP and subnet mask to use because there is no DHCP server.



Windows uses the following information to identify your computer on the network. You may change the name for this computer and the workgroup or domain that it will appear in.

Computer Name: CARIBOU

Workgroup: WORKGROUP

Figure 8-14 Configuring Windows NT 4.0

11. If asked for it, insert the Windows NT Workstation 4.0 CD-ROM and specify the path to the CD-ROM and \I386 folder, such as **D:\I386**, or obtain the installation files from the \I386 folder on your hard drive. Click **Continue**. If Remote Access Service (RAS) is installed, Windows NT will ask if you want to install TCP/IP for it; click **No** for this project exercise.
12. Click **Close** in the Network dialog box to bind the protocol to the NIC.
13. If you specified in Step 10 that you are not using DHCP, then the Microsoft TCP/IP dialog box appears. Make sure that **Specify an IP address** is selected, and enter the IP address and subnet mask obtained from your instructor (advance from field to field by pressing the period key).
14. Click **OK**.
15. Click **Yes** to restart the computer.
16. Click **OK** and click **Close**.

Note

Windows NT Server 4.0 is configured using the same steps as for Windows NT Workstation 4.0.

Project 8-7

In this hands-on project, you practice configuring RIS computer naming conventions by domain. RIS should be installed and configured prior to trying this project. Log on as

Administrator or using Administrator privileges. Also, find out from your instructor the location and name of the RIS server in the Active Directory.

To configure computer naming:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Double-click the domain that contains the RIS server, and find the server's name in the Active Directory tree, for example under Domain Controllers or Computers.
3. Right-click the RIS server and click **Properties**. Click the **Remote Install** tab. Notice the options available on this tab and record your observations.
4. Click the **Advanced Settings** button. Record the names of the tabs that you see and note their functions.
5. Click the **New Clients** tab, if it is not already displayed, and then click the **Customize** button.
6. In the Format box, enter **%1First%Last**. This sets up the naming convention to be the user's first initial combined with the last name. Notice the other variables that are described in the Computer Account Generation box and record them along with examples of their use in your lab journal or in a word-processed document.
7. Click **OK**.
8. Click **The following directory service location** and then click **Browse**.
9. Double-click the domain for which you want to establish the computer naming convention and double-click **Computers** under the domain. Click **OK**.
10. Click **OK**.
11. Click **OK** and then close the Active Directory Users and Computers tool.

CASE PROJECT

Aspen Consulting Project: Configuring Clients

This week you are working with Stanley & Bernstein Associates, which is an architectural firm that designs high-rise apartments and lofts and specializes in building these structures in city locations that are experiencing renovation. The firm also designs professional buildings in suburban areas, such as office buildings for medical and dental professionals. Stanley & Bernstein employs 72 people, who are members of four company units: the architects unit, the graphics design unit, the business unit, and the computer and technology support unit. Each unit is managed by a supervisor, and the supervisors compose a management group along with the two managing partners, Martin Stanley and Sharon Bernstein. You have already installed two Windows 2000 servers on the firm's network, configured both for TCP/IP, installed the Active Directory, and created a domain called Buildit.

1. Before creating accounts for users, your first recommendation is to meet with the management group and to plan an account naming convention and account policies.

What factors will you discuss with the group to help them make decisions? Include the following in your discussion:

- Account naming guidelines
- Account password policies
- Account lockout policies
- Other account security measures

2. The management group wants to make sure that you train the computer and technology support unit on how to configure the Active Directory. For now, they ask you to develop a set of instructions showing how to set up password and lockout policies.
3. The computer and technology support unit is impressed by the instructions you developed in Assignment 2, and now they ask you to prepare general instructions showing how to set up an account.
4. Before the firm starts setting up accounts, the manager's group has decided to decentralize this function and have each unit's supervisor be responsible for account management. The computer and technology group has already provided the supervisors with the account setup instructions, but they want to know what other steps should be taken to delegate account setup to the supervisors.
5. The computer and technology group has decided to create roaming profiles for all users. How can they do this, and how does this plan affect the information you provided in Assignments 3 and 4?
6. The managers group will be the first to access the new servers, and each person in this group will have a workstation that runs Windows 2000 Professional; the plan is to eventually upgrade all users to have Windows 2000 Professional. Explain how to use RIS to install Windows 2000 Professional over the network instead of purchasing separate CD-ROMs for each installation. Also, the two managing partners have very sensitive accounts that they want to access only from the computers in their offices. Explain how to accommodate this need.

Optional Case Assignments for Teams

Team Case One

Mark Arnez realizes that there are many advantages to using the Active Directory, but that it may not be appropriate for all types of organizations. He asks you to form a group and to develop a list of pros and cons for installing the Active Directory, considering the options available for setting up accounts, and for managing accounts, account policies, and security.

Team Case Two

Much has been in the news lately about productivity and the cost of doing business. Your firm is looking into the ways in which the use of profiles and group policies can lower the TCO of an organization. Form a group and develop two or three scenarios that illustrate how using profiles and group policies can reduce costs and increase users' productivity.